Chapter 8
Automated Information Systems (AIS)

Section 1. Responsibilities

8-100. Introduction

a. **Purpose and Scope.** This chapter addresses the protection and control of information processed on AIS. ***This entire chapter is contractor required and is not an option. The type is not bold or italicized, because it would include the complete chapter.*** AISS typically consist of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. This chapter specifies requirements and assurances for the implementation, operation, maintenance, and management of secure AIS used in support of SAP activities. Prior to using an AIS or AIS network for processing U.S. Government, Customer, or Program information, the Contractor/ Provider will develop an AIS Security Plan (AISSP) as described herein and receive written Customer authorization to process Customer information. Such authorization to process requires approval by the Customer. The Provider will also assign an Information System Security Representative (ISSR) to support the preparation of these documents and to subsequently manage AIS security on-site for the Customer's program. After the AISSP is approved by the Customer, the Provider will thereafter conform to the plan for all actions related to the Customer's program information. This information includes the selection, installation, test, operation, maintenance, and modification of AIS facilities, hardware, software, media, and output.

b. **Requirements.** The AISSP selected menu upgrades to the NISPOM baseline will be tailored to the Provider's individual AIS configuration and processing operations. Alternatives to the protective measures in this Supplement may be approved by the Customer after the Provider demonstrates that the alternatives are reasonable and necessary to accommodate the Customer's needs. Prior to implementation, the Provider will coordinate any envisioned changes or enhancements with the Customer. Approved changes will be included in the AISSP. Any verbal approvals will subsequently be documented in writing. The information and guidance needed to prepare and obtain approval for the AISSP is described herein.

c. Restrictions. No personally owned AISS will be used to process classified information.

8-101. Responsibilities.

The Customer is the Government organization responsible for sponsoring and approving the classified and/or unclassified processing. The Provider is the Contractor who is responsible for accomplishing the processing for the Customer. The Information System Security Representative (ISSR) is the Provider-assigned individual responsible for on-site AIS processing for the Customer in a secure manner.

a. **Provider Responsibilities.** The Provider will take those actions necessary to meet with the policies and requirements outlined in this document. The provider will:

(1) Publish and promulgate a corporate AIS Security Policy that addresses the classified processing environment.

(2) Designate an individual to act as the ISSR.

(3) Incorporate AISS processing Customer information as part of a configuration management program.

(4) Enforce the AIS Security Policy.

b. **ISSR Responsibilities.** The Provider-designated ISSR has the following responsibilities:

(1) AIS Security Policy. Implement the AIS Security Policy.

(2) AIS Security Program. Coordinate the establishment and maintenance of a formal AIS Security Program to ensure compliance with this document:

(a) AIS Security Plan (AISSP). Coordinate the preparation of an AISSP in accordance with the outline and instructions provided in this document. After Customer

approval, the AISSP becomes the controlling security document for AIS processing Customer information. Changes affecting the security of the AIS must be approved by the Customer prior to implementation and documented in the AISSP.

(b) AIS Technical Evaluation Test Plans. For systems operating in the compartmented or multi-level modes, prepare an AIS Technical Evaluation Test Plan in coordination with the Customer and applicable security documents.

(c) Certification. Conduct a certification test in accordance with 8-102, c. and provide a certification report.

(d) Continuity of Operations Plan (COOP). When contractually required, coordinate the development and maintenance of an AIS COOP to ensure the continuation of information processing capability in the event of an AIS-related disaster resulting from fire, flood, malicious act, human error, or any other occurrence that might adversely impact or threaten to impact the capability of the AIS to process information. This plan will be referenced in the AISSP.

(e) Documentation. Ensure that all AIS security-related documentation as required by this chapter is current and is accessible to properly authorized individuals.

(f) Customer Coordination. Coordinate all reviews, tests, and AIS security actions.

(g) Auditing. Ensure that the required audit trails are being collected and reviewed as stated in 8-303.

(h) Memorandum of Agreement. As applicable, ensure that Memoranda of Agreement are in place for AISS supporting multiple Customers.

(i) Compliance Monitoring. Ensure that the system is operating in compliance with the AISSP.

(j) AIS Security Education and Awareness. Develop an on-going AIS Security Education and Awareness Program.

(k) Abnormal Occurrence. Advise Customer in a timely manner of any abnormal event that affects the security of an approved AIS.

(1) Virus and malicious code. Advise Customer in a timely manner of any virus and malicious code on an approved AIS.

(3) Configuration Management. Participate in the configuration management process.

(4) Designation of Alternates. The ISSR may designate alternates to assist in meeting the requirements outlined in the chapter.

c. Special Approval Authority. In addition to the above responsibilities, the Customer may authorize in writing an ISSR to approve specific AIS security actions including:

(1) Equipment Movement. Approve and document the movement of AIS equipment.

(2) Component Release. Approve the release of sanitized components and equipment in accordance with Tables 1 and 2 in 8-501.

(3) Stand-alone Workstation and Portable AIS Approval. Approve and document new workstations in accordance with an approved AIS security plan and the procedures defined in this document for workstations with identical functionality. Approve and document portable AIS.

(4) Dedicated and System High Network Workstation Approval. Approve and document additional workstations identical in functionality to existing workstations on an approved Local Area Network (LAN) provided the workstations are not located outside of the previously defined boundary of the LAN.

(5) Other AIS Component Approval. Approve and document other AIS components identical in functionality to existing components on an approved LAN provided the components are not located outside of the previously defined boundary of the LAN.

8-102. Approval To Process.

Prior to using any AIS to process Customer information, approval will be obtained from the Customer. The following requirements will be met prior to approval.

a. **AIS Security Program.** The Provider will have an AIS security program that includes:

(1) An AIS security policy and a formal AIS security structure to ensure compliance with the guidelines specified in this document;

(2) An individual whose reporting functionalities are within the Provider's security organization formally named to act as the ISSR;

(3) The incorporation of AISs processing Customer information into the Provider's configuration management program. The Provider's configuration management program shall manage changes to an AIS throughout its life cycle. As a minimum the program will manage changes in an AIS's:

(a) Hardware components (data retentive only)

(b) Connectivity (external and internal)

(c) Firmware

(d) Software

(e) Security features and assurances

(f) AISSP

(g) Test Plan

(4) Control. Each AIS will be assigned to a designated custodian (and alternate custodian) who is responsible for monitoring the AIS on a continuing basis. The custodian will ensure that the hardware, installation, and maintenance as applicable conform to appropriate requirements. The custodian will also monitor access to each AIS. Before giving users access to any such AIS, the custodian will have them sign a statement indicating their awareness of the restrictions for using the AIS. These statements will be maintained on file and available for review by the ISSR.

b. **AIS Security Plan (AISSP). The** Provider will prepare and submit an AISSP covering AISS processing information in a Customer's Special Access Program Facility (SAPF), following the format in Appendix C. For RD, the Customer may modify the AISSP format.

c. AIS Certification and Accreditation.

(1) Certification. Certification is the comprehensive evaluation of technical and non-technical security features to establish the extent to which an AIS has met the security requirements necessary for it to process the Customer information. Certification precedes the accreditation. The certification is based upon an inspection and test to verify that the AISSP accurately describes the AIS configuration and operation (See Appendix C and D). A Certification Report summarizing the following will be provided to the Customer:

(a) For the dedicated mode of operation, the provider must verify that access controls, configuration management, and other AISSP procedures are functional.

(b) In addition, for System High AIS the ISSR will verify that discretionary controls are implemented.

(c) For compartmented and multilevel AIS, certification also involves testing to verify that technical security features required for the mode of operation are functional. Compartmented and multi-level AIS must have a Technical Evaluation Test Plan that includes a detailed description of how the implementation of the operating system software, data management system software, firmware, and related security software packages will enable the AIS to meet the Compartmented or Multilevel Mode requirements. The plan outlines the inspection and test procedures to be used to demonstrate this compliance.

(2) Accreditation. Accreditation is the formal declaration by the Customer that a classified AIS or network is approved to operate in a particular security mode; with a prescribed set of technical and non-technical security features; against a defined threat; in a given operational environment; u rider a stated operational concept; with stated interconnections to other AIS; and at an acceptable level of risk. The accreditation decision is subject to the certification process. Any changes to the accreditation criteria described above may require a new accreditation.

d. **Interim Approval.** The Customer may grant an interim approval to operate.

e. Withdrawal of Accreditation. The Customer may withdraw accreditation if:

(1) The security measures and controls established and approved for the AIS do not remain effective.

(2) The AIS is no longer required to process Customer information.

f. **Memorandum of Agreement.** A Memorandum of Agreement (MOA) is required whenever an accredited AIS is co-utilized, interfaced, or networked between two or more Customers. This document will be included, as required, by the Customer.

g. Procedures for Delegated Approvals. For AISS operating in the dedicated or system high modes, the Customer may delegate special approval authority to the ISSR for additional AISS that are identical in design and operation. That is: two or more AIS are identical in design and operate in the same security environment (same mode of operation, process information with the same sensitivities, and require the same accesses and clearances, etc). Under these conditions the AISSP in addition to containing the information required by Appendix C shall also include the certification requirements (inspection and tests) and procedures that will be used to accredit all AISs. The CSA will validate that the certification requirements are functional by accrediting the first AIS using these certification requirements and procedures. The ISSR may allow identical AIS to operate under that accreditation if the certification procedures are followed and the AIS meets all the certification requirements outline in the AISSP. The AISSP will be updated with the identification of the newly accredited AIS and a copy of each certification report will be kept on file.

8-103. Security Reviews.

a. **Purpose.** Customer AIS Security Reviews are conducted to verify that the Provider's AIS is operated in accordance with the approved AISSP.

b. **Scheduling.** Customer AIS Reviews are normally scheduled at least once every 24 months for Provider systems processing Customer program information. The Customer will establish specific review schedules.

c. Review Responsibilities. During the scheduled Customer AIS Security Review, the Provider will furnish the Customer representative conducting the Review with all requested AIS or network documentation. Appropriate Provider security, operations, and management representatives will be made available to answer questions that arise during the Customer AIS Review process.

d. **Review Reporting.** At the conclusion of the Customer AIS Review visit, the Customer will brief the Provider's appropriate security, operations, and management representatives on the results of the Review and of any discrepancies discovered and the recommend measures for correcting the security deficiencies. A formal report of the Customer AIS Review is provided to the Provider's security organization no later than 30 days after the Review.

e. Corrective Measures. The Provider will respond to the Customer in writing within 30 days of receipt of the formal report of deficiencies found in the Customer AIS Review process. The response will describe the actions taken to correct the deficiencies outlined in the formal report of Customer AIS Review findings. If proposed actions will require an expenditure in funds, approval will be obtained from the Contracting Officer prior to implementation.

Section 2. Security Modes

8-200. Security Modes-General.

a. AISs that process classified information must operate in the **dedicated,** system high, **compartmented,** or multilevel mode. **Security** modes are authorized variations in security environments, **requirements,** and methods of operating. In all modes, the integration of automated and conventional security measures **shall,** with reasonable dependability, prevent unauthorized access to classified information during, or resulting from, the processing, storage, or transmission of such information, and prevent unauthorized manipulation of the AIS that could result in the compromise or loss of classified information.

b. In determining the mode of operation of an AIS, three elements must be addressed: the boundary and perimeter of the AIS, the nature of the data to be processed, and the level and diversity of access privileges of intended users. Specifically:

(1) The boundary of an AIS includes all users that are directly or indirectly connected and who can receive data from the AIS without a reliable human review by an appropriately cleared authority. The perimeter is the extent of the AIS that is to be **accredited** as a single entity.

(2) The nature of data is defined in terms of its **classification levels,** compartments, **subcompartments,** and sensitivity levels.

(3) The **level** and diversity of access privileges of its users are defined as their clearance levels, **need**-to-know, and formal access approvals.

8-201. **Dedicated** Security **Mode.**

a. An AIS is operating in the dedicated mode (processing either full time or for a specified period) when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has **all** of the following:

(1) A valid personnel clearance for all information stored or processed on the AIS.

(2) Formal access approvals and **has** executed all appropriate non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or SAPS).

(3) A valid need to know for all information stored on or processed within the AIS.

b. The following security requirements are established for AISS operating in the **dedicated** mode:

(1) Be **located** in a **SAPF.**

(2) Implement and **enforce** access procedures to the **AIs.**

(3) **All** hard copy output will be handled at the level for which the system is accredited until reviewed by a knowledgeable individual.

(4) **All** media removed from the system will **be** protected at the highest classification level of information stored or processed on the system until reviewed and properly marked according to procedures in the AIS **security** plan.

c. **Security Features for Dedicated Security Mode.**

(1) Since the system is not required to provide technical security features, it is up to the user to **protect** the information on the system. For networks operating in the dedicated mode, automated identification and authentication controls are required.

(2) For DoD, the Customer may require audit records of user access to the system. Such records will include: user ID, start date and time, and stop date and time. Logs will be maintained IAW 8-303.

d. **Security Assurances for Dedicated Security Mode.**

(1) AIS *security* assurances must *include* an approach for specifying, documenting, **controlling,** and maintaining the integrity of all appropriate AIS hardware, firmware, software, communicant ions interfaces, operating *procedures,* installation structures, security documentation, and changes thereto.

(2) Examination of Hardware and Software. Classified AIS hardware and software shall be examined when received from the vendor and before being placed into use.

(a) Classified AIS Hardware. An examination shall result in assurance that the equipment appears to be in good working order and have no parts that might be detrimental to the secure operation of the resource. Subsequent changes and developments which affect security may require additional examination.

(b) Classified AIS Software.

1. Commercially procured software shall be examined to assure that the software contains no features which might be detrimental to the security of the classified AIS.

2. Security-related software shall be examined to assure that the security features function as specified.

(c) Custom Software or Hardware Systems. New or significantly changed security relevant software and hardware developed specifically for the system shall be subject to testing and review at appropriate stages of development.

8-202. **System High Security Mode.**

a. An AIS is operating in the system high mode (processing either full time or for a specified period) when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid personnel clearance for ail information on the AIS.

(2) Formal access approval and has signed non-disclosure agreements for all the information stored and/or processed (including all compartments and subcompartments).

(3) A valid need-to-know for some of the information contained within the system.

b. AISS operating in the system high mode, in addition to meeting all of the security requirements, features, and assurances established for the dedicated mode, will meet the following:

(1) Security Features for System High Mode

(a) Define and control access between system users and named objects (e.g., files and programs) ‘in the AIS. The enforcement mechanism must allow system users to specify and control the sharing of those objects by named individuals and/or explicitly defined groups of individuals. The access control mechanism must, either by explicit user action or by default, provide that all objects are protected from unauthorized access (discretionary access control). Access permission to an object by users not already possessing access permission must only be assigned by authorized users of the object.

(b) Time Lockout. Where technically feasible, the AIS shall time lockout an interactive session after an interval of user inactivity. The time interval and restart requirements shall be specified in the AIS Security Plan.

(c) Audit Trail. Provide an audit trail capability that records time, date user ID, terminal ID (if applicable), and file name for the following events:

1. Introduction of objects into a user’s address space (e.g., file open and program initiation as determined by the Customer and ISSR).

2. Deletion of objects (e.g., as determined by the Customer and ISSR).

3. System log-on and log-off

4. Unsuccessful access attempts.

(d) Require that memory and storage contain no residual data from the previously contained object before being assigned, allocated, or reallocated to another subject.

(e) Identification Controls. Each person having access to a classified AIS shall have the proper security clearances and authorizations and be uniquely identified and authenticated before access to the classified AIS is permitted. The identification and authentication methods used shall be specified and approved in the AIS Security Plan. User access controls in classified AISS shall include authorization, user

in the AIS Security Plan. User access controls in classified AISS shall include authorization, user identification, and authentication administrative controls for assigning these shall be covered in the AISSP.

1. User Authorizations. The manager or supervisor of each user of a classified AIS shall determine the required authorizations, such as need-to-know, for that user.

2. User Identification. Each system user shall have a unique user identifier and authenticator.

   a. User ID Removal. The ISSR shall ensure the development and implementation of procedures for the prompt removal of access from the classified AIS when the need for access no longer exists.

   b. User ID Revalidation. The AIS ISSR shall ensure that all user IDs are revalidated at least annually, and information such as sponsor and means of 'off-line contact (e.g., phone number, mailing address) are updated as necessary.

(f) Authentication. Each user of a classified AIS shall be authenticated before access is permitted. This authentication can be based on any one of three types of information: something the person knows (e.g., a password); something the person possesses (e.g., a card or key); something about the person (e.g., fingerprints or voiceprints); or some combination of these three. Authenticators that are passwords shall be changed at least every six months.

1. Requirements.

   a. Log-on. Users shall be required to authenticate their identities at "log-on" time by supplying their authenticator (e.g., password, smart card, or fingerprints) in conjunction with their user ID.

   b. Protection of Authenticator. An Authenticator that is in the form of knowledge or possession (password, smart card, keys) shall not be shared with anyone. Authenticators shall be protected at a level commensurate with the accreditation level of the Classified AIS.

2. Additional Authentication Countermeasures. Where the operating system provides the capability, the following features shall be implemented:

   a. Log-on Attempt Rate. Successive log-on attempts shall be controlled by denying access after multiple (maximum of five) unsuccessful attempts on the same user ID; by limiting the number of access attempts in a specified time period; by the use of a time delay control system; or other such methods, subject to approval by the Customer.

   b. Notification to the User. The user shall be notified upon successful log-on of: the date and time of the user's last log-on; the ID of the terminal used at last log-on; and the number of unsuccessful log-on attempts using this user ID since the last successful log-on. This notice shall require positive action by the user to remove the notice from the screen.

(g) The audit, identification, and authentication mechanisms must be protected from unauthorized access, modification, or deletion.

   c. Security Assurances for System High Mode. The system security features for need-to-know controls will be tested and verified. Identified flaws will be corrected.

8-203. **Compartmented Security Mode.**

a. An AIS is operating in the compartmented mode when users with direct or indirect access to the AIS,

its peripherals, or remote terminals have all of the following:

(1) A valid personnel clearance for access to the most restricted information processed in the AIs.

(2) Formal access approval and have signed nondisclosure agreements for that information to which he/she is to have access (some users do not have formal access approval for all compartments or subcompartments processed by the AIS.)

(3) A valid need-to-know for that information for which he/she is to have access.

b. **Security Features for Compartmented Mode. In** addition to all Security Features and Security Assurances required for the System High Mode of Operation, Classified AIS operating in the Compartmented Mode of Operation shall also include:

(1) Resource Access Controls,

(a) Security Labels. The Classified AIS shall place security labels on all entities (e.g., files) reflecting the sensitivity (classification level, classification category, and handling caveats) of the information for resources and the authorizations (security clearances, need-to-know, formal access approvals) for users. These labels shall be an integral part of the electronic data or media. These security labels shall be compared and validated before a user is granted access to a resource.

(b) Export of Security Labels. Security labels exported from the Classified AIS shall be accurate representations of the corresponding security labels on the information in the originating Classified AIS.

(2) Mandatory Access Controls. Mandatory access controls shall be provided. These controls shall provide a means of restricting access to files based on the sensitivity (as represented by the label) of the information contained in the files and the formal authorization (i.e., security clearance) of users to access information of such sensitivity.

(3) No information shall be accessed whose compartment is inconsistent with the session log-on.

(4) Support a trusted communications path between itself and each user for initial log-on and verification.

(5) Enforce, under system control, a system-generated, printed, and human-readable security classification level banner at the top and bottom of each physical page of system hard-copy output.

(6) Audit these additional events: the routing of all system jobs and output, and changes to security labels.

(7) Security Level Changes. The system shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A user shall be able to query the system as desired for a display of the user's complete sensitivity label.

c. Security Assurances for Compartmented Mode.

(I) Confidence in Software Source. In acquiring resources to be used as part of a Classified AIS, consideration shall be given to the level of confidence placed in the vendor to provide a quality product, to support the security features of the product, and to assist in the correction of any flaws.

(2) Flaw Discovery. The Provider shall ensure the vendor has implemented a method for the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security of the AIS.

(3) No Read Up, No Write Down. Enforce an upgrade or downgrade principle where all users processing have a system-maintained classification; no data is read that is classified higher than the processing session authorized; and no data is written unless its security classification level is equal to or lower than the user's authorized processing security classification and all non-hierarchical categories are the same.

(4) Description of the Security Support Structure (often referred to as the Trusted Computing Base). The protections and provisions of the security support structure shall be documented in such a manner to show the underlying planning for the security of a Classified AIS. The security enforcement mechanisms shall be isolated and protected from any user or unauthorized process interference or modification.

Hardware and software features shall be provided that can be used to periodically validate the correct operation of the elements of the security enforcement mechanisms.

(5) Independent Validation and Verification. An Independent Validation and Verification team shall assist in the technical evaluation testing of a classified AIS and shall perform validation and verification testing of the system as required by the Customer.

(6) Security Label Integrity. The methodology shall ensure the following:

(a) Integrity of the security labels;

(b) The association of a security label with the transmitted data; and

(c) Enforcement of the control features of the security labels.

(7) Detailed Design of security enforcement mechanisms. An informal description of the security policy model enforced by the system shall be available.

8-204. **Multilevel Security** Mode. NOTE: Multilevel Security Mode is not routinely -authorized for SCI or SAP applications. Exceptions for SCI may be made by the heads of CIA, DIA, or NSA on a case-by-case basis. Exceptions for SAP may be made by the Customer.

a. An AIS is operating in the multilevel mode when all of the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

(1) Some users do not have a valid personnel clearance for all of the information processed in the AIS. (Users must possess a valid CONFIDENTIAL, SECRET, or TOP SECRET clearance.)

(2) All users have the proper clearance and have the appropriate access approval (i.e., signed nondisclosure agreements) for that information to which they are intended to have access.

(3) All have a valid need-to-know for that information to which they are intended to have access.

b. Security **Features for Multilevel Mode.** In addition to all security features and security assurances required for the compartmented mode of operation, classified AIS operating in the multilevel mode of operation shall also include:

(1) Audit. Contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.

(2) Trusted Path. Support a trusted communication path between the AIS and users for use when a positive AIS-to-user connection is required (i.e., log-on, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the AIS and shall be logically isolated and unmistakably distinguishable from other paths. For Restricted Data, this requirement is only applicable to multilevel AIS that have at least one uncleared user on the AIS.

(3) Support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The AIS system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrative role on the AIS system. Non-security functions that can be performed in the security administrative role shall be limited strictly to those essential to performing the security role effectively.

(4) Security Isolation. The AIS security enforcement mechanisms shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the security enforcement mechanisms shall provide isolation and noncircumvention of isolation functions. For Restricted Data, this requirement is only applicable to multilevel AIS that have at least one uncleared user on the AIS.

(5) Protection of Authenticator. Authenticators shall be protected at the same level as the information they access.

c. Security Assurances for Multilevel Mode.

(1) Flaw Tracking and Remediation. The Provider shall ensure the vendor provides evidence that all discovered flaws have been tracked and remedied.

(2) Life-Cycle Assurance. The development of the Classified AIS hardware, firmware, and software shall be under life-cycle control and management (i.e., control of the Classified AIS from the earliest design stage through decommissioning).

(3) Separation of Functions. The functions of the AIS ISSR and the Classified AIS manager shall not be performed by the same person.

(4) Device Labels. The methodology shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.

(5) Security Penetration Testing. In addition to testing the performance of the classified AIS for certification and for ongoing testing, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and for ongoing testing.

(6) Trusted Recovery. Provide procedures and/or mechanisms to assure that, after an AIS system failure or other discontinuity, recovery without a protection compromise is obtained.

(7) Covert Channels. A covert channel analysis shall be performed.

Section 3. System Access and Operation

8-300 System Access. Access to the system will be limited to authorized personnel. Assignment of AIS access and privileges will be coordinated with the ISSR. Authentication techniques must be used to provide control for information on the system. Examples of authentication techniques include, but are not limited to: passwords, tokens, biometrics, and smart cards. User authentication techniques and procedures will be described in the AISSP.

a. **User IDs.** User IDs identify users in the system and are used in conjunction with other authentication techniques to gain access to the system. User IDs will be disabled whenever a user no longer has a need-t-know. The user ID will be deleted from the system only after review of programs and data associated with the ID. Disabled accounts will be removed from the system as soon as practical. Whenever possible, access attempts will be limited to five tries. Users who fail to access the system within the established limits will be denied access until the user ID is reactivated.

b. **Access Authentication.**

(1) Password. When used, system log-on passwords will be randomly selected and will be at least six characters in length. The system log-on password generation routine must be approved by the Customer.

(2) Validation. Authenticators must be validated by the system each time the user accesses the AIS.

(3) Display. System log-on passwords must not be displayed on any terminal or contained in the audit trail. When the AIS cannot prevent a password from being displayed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(4) Sharing. Individual user authenticators (e.g., passwords) will not be shared by any user.

(5) Password Life. Passwords must be changed at least every six months.

(6) Compromise. Immediately following a suspetted or known compromise of a password or Personal Identification Number (PIN) the ISSR will be notified and a new password or PIN issued.

(7) Group Log-on Passwords. Use of group log-on passwords must be justified and approved by the Customer. After log-on, group passwords may be used for file access.

c. **Protection of Authenticators.** Master data files containing the user population system log-on authenticators will be encrypted when practical. Access to the files will be limited to the ISSR and designated alternate(s), who will be identified in writing.

d. **Modems.** Modems require Customer approval prior to connection to an AIS located in a Customer SAPF.

e. **User Warning Notice.** The Customer may require log-on warning banners be installed.

8-301. System Operation.

a. Processing initialization is the act of changing the AIS from unclassified to classified, from one classified processing level to another, or from one compartment to another or from one Customer to another. To begin processing classified information on an approved AIS the following procedures must be implemented:

(1) Verify that prior mode termination was properly performed.

(2) Adjust the area security controls to the level of information to be processed.

(3) Configure the AIS as described in the approved AISSP. The use of logical disconnects requires Customer approval.

(4) Initialize the system for processing at the approved level of operation with a dedicated copy of the operating system. This copy of the operating system must be labeled and controlled commensurate with the security classification and access levels of the information to be processed during the period.

b. **Unattended Processing.** Unattended processing will have open storage approval and concurrence from the customer. Prior to unattended processing,

all remote input and/or output (1/0) not in approved open storage areas will be physically or electrically disconnected from the host CPU. The disconnect will be made in an area approved for the open storage. Exceptions are on a case-by-case basis and will require Customer approval.

c. **Processing Termination.** Processing termination of any AIS will be accomplished according to the following requirements.

(1) Peripheral Device Clearing. Power down all connected peripheral devices to sanitize all volatile buffer memories. Overwriting of these buffer areas will be considered by the Customer on a case-by-case basis.

(2) Removable Storage Media. Remove and properly store removable storage media.

(3) Non-removable (Fixed) Storage Media. Disconnect (physically or electrical] y) all storage devices with nonremovable storage media not designated for use during the next processing period.

(4) CPU Memory. Clear or sanitize as appropriate all internal memory including buffer storage and other reusable storage devices (which are not disabled, disconnected, or removed) in accordance with 8-501, Table 2.

(5) Laser Printers. Unless laser printers operating in SAPFS will operate at the same classification level with the same access approval levels during the subsequent processing period, they will be cleared by running three pages of unclassified randomly generated text. For SCI, five pages of unclassified pages will be run to clear the printer. These pages will not include any blank spaces or solid black areas. Otherwise, no pages need be run through the printer at mode termination.

(6) Thermal printers. Thermal printers have a thermal film on a spool and take-up reel. Areas in which these types of laser printers are located will be either approved for open storage, or the spools and take-up reels will be removed and placed in secure storage. The printer must be sanitized prior to use at a different classification level.

(7) Impact-type Printers. Impact-type printers (e.g., dot-matrix) in areas not approved for open storage will be secured as follows: Remove and secure all printer ribbons or dispose of them as classified trash. Inspect all printer platens. If any indication' of printing is detected on the platen, then the platen will be either cleaned to remove such printing or removed and secured in an approved classified container.

(8) Adjust area security controls.

8-302. **Collocation of Classified and Unclassified AIS.**

a. Customer permission is required before a Provider may collocate unclassified AIS and classified AIS. This applies when:

(1) The unclassified information is to be processed on an AIS located in a SAPF, or

(2) The unclassified information is resident in a database located outside of a SAPF but accessed from terminals located within the SAPF.

b. AIS approved for processing unclassified information will be clearly marked for UNCLASSIFIED USE ONLY when located within a SAPF. In addition the following requirements apply:

(I) Must be physically separated from any classified AIS.

(2) Cannot be connected to the classified AIS.

(3) Users shall be provided a special awareness briefing.

(4) ISSR must document the procedures to ensure the protection of classified information.

(5) All unmarked media is assumed to be classified until reviewed and verified.

c. Unclassified portable AIS devices are prohibited in a SAPF unless Customer policy specifically permits their use. If permitted, the following procedures must be understood and followed by the owner and user:

(1) Connection of unclassified portable AIS to classified AIS is prohibited.

(2) Connection to other unclassified AISs may be allowed provided Customer approval is obtained.

(3) Use of an internal or external modem with the AIS device is prohibited within the SAPF.

(4) The Provider will incorporate these procedures in the owner's initial and annual security briefing.

(5) Procedures for monitoring portable AIS devices within the SAPF shall be outlined in either the AISSP or the Facility Security Plan. These devices and the data contained therein are subject to security inspection by the ISSR and the Customer. Procedures will include provisions for random reviews of such devices to ensure that no classified program-specific or program-sensitive data is allowed to leave the secure area. Use of such a device to store or process classified information may, at the discretion of the Customer, result in confiscation of the device. All persons using such devices within the secure area will be advised of this policy during security awareness briefings.

(6) Additionally, where Customer policy permits, personally owned portable AIS devices may be used for unclassified processing only and must follow the previous guidelines.

8-303. System **Auditing.**

a. **Audit Trails.** Audit trails provide a chronological record of AIS usage and system support activities related to classified or sensitive processing. In addition to the audit trails normally required for the operation of a stand-alone AIS, audit trails of network activities will also be maintained. Audit trails will provide records of significant events occurring in the AIS in sufficient detail to facilitate reconstruction, review, and examination of events involving possible compromise. Audit trails will be protected from unauthorized access, modification, and deletion. Audit trail requirements are described under mode of operation.

b. **Additional Records and Logs. The** following additional records or logs will be maintained by the Provider regardless of the mode of operation. These will include:

(1) Maintenance and repair of AIS hardware, including installation or removal of equipment, devices, or components.

(2) Transaction receipts, such as equipment sanitization, release records, etc.

(3) Significant AIS changes (e.g., disconnecting or connecting remote terminals or devices, AIS upgrading or downgrading actions, and applying seals to or removing them from equipment or device covers).

c. Audit Reviews. The audit trails, records, and logs created during the above activities will be reviewed and annotated by the ISSR (or designee) to be sure that all pertinent activity is proper] y recorded and appropriate action has been taken to correct anomalies. The Customer will be notified of all anomalies that have a direct impact on the security posture of the system. The review will be conducted at least week] y.

d. **Record Retention.** The Provider will retain the most current 6 to 12 months (Customer Option) of records derived from audits at all times. The Customer may approve the periodic use of data reduction techniques to record security exception conditions as a means of reducing the volume of audit data retained. Such reduction will not result in the loss of any significant audit trail data.

Section 4. Networks

8-400 Networks. This section addresses network-specific requirements that are in addition to the previously stated AIS requirements. Network operations must preserve the security requirements associated with the AIS's mode of operation.

a. Types of Networks.

(1) A unified network is a collection of AIS's or network systems that are accredited as a single entity by a single CSA, A unified network may be as simple as a small LAN operating in dedicated mode, following a single security policy, accredited as a single entity, and administered by a single ISSR. The perimeter of such a network encompasses all its hardware, software, and attached devices. Its boundary extends to all its users. A unified network has a single mode of operation. This mode of operation will be mapped to the level of trust required and will address the risk of the least trusted user obtaining the most sensitive information processed or stored on the network.

(2) An interconnected network is comprised of separately accredited AISs and/or unified networks. Each self-contained AIS maintains its own intra-AIS services and controls, protects its own resources, and retains its individual accreditation. Each participating AIS or unified network has its own ISSR. The interconnected network must have a security support structure capable of adjudicating the different security policy (implementations) of the participating AISS or unified net works. An interconnected network requires accreditation, which may be as simple as an addendum to a Memorandum of Agreement (MOA) between the accrediting authorities.

b. **Methods of Interconnection.**

(1) Security Support Structure (SSS) is the hardware, software, and firmware required to adjudicate security policy and implementation differences between and among connecting unified networks and/or AISs. The SSS must be accredited. The following requirements must be satisfied as part of the SSS accreditation:

(a) Document the security policy enforced by the SSS.

(b) Identify a single mode of operation.

(c) Document the network security architecture and design.

(d) Document minimum contents of MOA's required for connection to the SSS.

(2) The interconnection of previously accredited systems into an accredited network may require a reexamination of the security features and assurances of the contributing systems to ensure their accreditations remain valid.

(a) Once an interconnected network is defined and accredited, additional networks or separate AISS (separately accredited) may only be connected through the accredited Sss.

(b) The addition of components to contributing unified networks which are members of an accredited interconnected network are allowed provided these additions do not change the accreditation of the contributing system.

c. **Network Security Management. The** Provider will designate an ISSR for each Provider network. The ISSR may designate a Network Security Manager (NSM) to oversee the security of the Provider's network(s), or may assume that responsibility. The ISSR is responsible for coordinating the establishment and maintenance of a formal network security program based on an understanding of the overall security-relevant policies, objectives, and requirements of the Customer. The NSM is responsible for ensuring day-to-day compliance with the network security requirements as described in the AISSP (as covered below) and this Supplement.

d. **Network Security Coordination.** When different accrediting authorities are involved, a Memorandum of Agreement is required to define the cognizant authority and the security arrangements that will govern the operation of the overall network. When

two or more ISSRS are designated for a network, a lead ISSR will be named by the Provider(s) to ensure a comprehensive approach to enforce the Customer's overall security policy.

e. Network Security.

The AISSP must address:

(1) A description of the network services and mechanisms that implement the network security policy.

(2) Consistent implementation of security features across the network components.

(a) Identification and Authentication Forwarding. Reliable forwarding of the identification shall be used between AISS when users are connecting through a network. When identification forwarding cannot be verified, a request for access from a remote AIS shall require authentication before permitting access to the system.

(b) Protection of Authenticator Data. In forwarding the authenticator information and any tables (e.g., password tables) associated with it, the data shall be protected from access by unauthorized users (e.g., encryption), and its integrity shall be ensured.

(c) Description of the network and any external connections.

(d) The network security policy including mode of operation, information sensitivities, and user clearances.

(e) Must address the internode transfer of information (e.g., sensitivity level, compartmentation, and any special access requirements), and how the information is protected.

(f) Communications protocols and their security features.

(g) Audit Trails and Monitoring.

1. If required by the mode of operation, the network shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of successful and unsuccessful accesses to the AIS network components within the perimeter of the accredited network. The audit data shall be protected so that access is limited to the ISSR or his/her designee.

2. For Restricted Data, methods of continuous on-line monitoring of network activities may be included in each network operating in the **Compartmented Securit** y Mode or higher. This monitoring may also include realtime notification to the ISSR of any system anomalies.

3. For Restricted Data networks operating in the Compartmented Mode or higher, the Customer may require the audit trail to include the changing of the configuration of the network (e.g., a component leaving the network or rejoining).

4. The audit trail records will allow association of the network activities with corresponding user audit trails and records.

5. Provisions shall be made and the procedures documented to control the loss of audit data due to unavailability of resources.

6. For Restricted Data, the Customer may require alarm features that automatically terminate the data **flow** in case of a malfunction and then promptly notify the ISSR of the anomalous conditions.

(h) Secure Message Traffic. The communications methodology for the network shall ensure the detection of errors in traffic across the network links.

f. **Transmission Security.** Protected Distribution Systems or National Security Agency approved encryption methodologies shall be used to protect classified information on communication lines that leave the SAPF. Protected distribution systems shall be either constructed in accordance with the national standards or utilize National Security Agency approved protected distribution systems.

g. Records. The Customer may require records be maintained of electronic transfers of data between automated information systems when those systems are not components of the same unified network. Such records may include the identity of the sender, identity and location of the receiver, date/time of the transfer, and description of the data sent. Records are retained according to 8-303.d.

Section 5. Software and Data Files

8-500. Software and Data Files.

a. **Acquisition and Evaluation.** ISSR approval will be obtained before software or data files may be brought into the SAPF. All software must be acquired from reputable and/or authorized sources as determined by the ISSR. The Provider will check all newly-acquired software or data files, using the most current version and/or available of virus checking software and procedures identified in the AISSP to improve assurance that the software or data files are free from malicious code.

b. Protection. Media that may be written to (e.g., magnetic media) must be safeguarded commensurate with the level of accreditation of the dedicated or system high AIS. Media on compartmented or multilevel AISS will be protected commensurate with the level of the operating session. If a physical write-protect mechanism is utilized, media may be introduced to the AIS and subsequently removed without changing the original classification. The integrity of the write-protection mechanism must be verified at a minimum of once per day by attempting to write to the media. Media which cannot be changed (e.g., CD read-only media) may be loaded onto the classified system without labeling or classifying it provided it is immediately removed from the secure area. If this media is to be retained in the secure area, it must be labeled, controlled, and stored as unclassified media as required by the Customer.

(1) System Software. Provider personnel who are responsible for implementing modifications to system or security-related software or data files on classified AISS inside the SAPF will be appropriately cleared. Soft ware that contains security related functions (e.g., sanitization, access control, auditing) will be validated to confirm that security-related features are fully functional, protected from modification, and effective.

(2) Application Software. Application software or data files (e.g., general business software), that will be used by a Provider during classified processing, may be developed/modified by personnel outside the security area without the requisite security clearance with the concurrence of the Customer.

(3) Releasing Software. Software that has not been used on an AIS processing classified information may be returned to a vendor. If media containing software (e.g., applications) are used on a classified system and found to be defective, such media may not he removed from a SAPF for return to a vendor. When possible, software will be tested prior to its introduction into the secure facility.

c. Targetability. For SCI and SAP the software, whether obtained from sources outside the facility or developed by Provider personnel, must be safeguarded to protect its integrity from the time of acquisition or development through its life cycle at the Provider's facility (i.e., design, development, operational, and maintenance phases). Uncleared personnel will not have any knowledge that the software or data files will be used in a classified area, although this may not be possible in all cases. Before software or data files that are developed or modified by uncleared personnel can be used in a classified processing period, it must be reviewed by appropriately cleared and knowledgeable personnel to ensure that no security vulnerabilities or malicious code exists. Configuration management must be in place to ensure that the integrity of the software or data files is maintained.

d. **Maintenance Software.** Software used for maintenance or diagnostics will be maintained within the secure computing facility and, even though unclassified, will be separately controlled. The AISSP will detail the procedures to be used.

e. **Remote Diagnostics.** Customer approval will be obtained prior to using vendor-supplied remote diagnostic links for on-line use of diagnostic software. The AISSP will detail the procedures to be used.

8-501. **Data Storage Media.** Data storage media will be control led and labeled at the appropriate classification level and access controls of the AIS unless write-protected in accordance with 8-500.b. Open storage approval will be required for non-removable media.

a. **Labeling Media.** All data storage media will be labeled in human-readable form to indicate its classification level, access controls (if applicable), and other identifying information. Data storage media that is to be used solely for unclassified processing

and collocated with classified media will be marked as UNCLASSIFIED. Color coding (i e., media, labels) is recommended. If required by the Customer, all removable media will be labeled with a classification label immediately after removing it from its factory-sealed container.

b. **Reclassification.** When the classification of the media increases to a higher level, replace the classification label with a higher classification-level label. The label will reflect the highest classification level, and access controls (if applicable) of any information ever stored or processed on the AIS unless the media is write-protected by a Customer-approved mechanism. Media may never be downgraded in classification without the Customer's written approval.

c. **Copying Unclassified Information from a Classified AIS.**

(1) **The** unclassified data will be written to factory-fresh or verified unclassified media using approved copying routines and/or utilities and/or procedures as stated in the AISSP. For SCI and SAP, media to be released will be verified by reviewing all data on the media including embedded text (e.g., headers and footers). Data on media that is not in human readable form (e.g., imbedded graphs, sound, video) will be examined for content with the appropriate software applications. Data that cannot be reasonably observed in its entirety will be inspected by reviewing random samples of the data on the media.

(2) Moving Classified Data Storage Media Between Approved Areas. The ISSR w il I establish procedures to ensure that data will be written to factory-fresh or sanitized media. The media will be reviewed to ensure that only the data intended was actually written and that it is appropriately classified and labeled. Alternatives for special circumstances may be approved by the Customer. All procedures will be documented in the AISSP.

d. **Overwriting, Degaussing, Sanitizing, and Destroying Media.** Cleared and sanitized media may be reused within the same classification level (i.e., TS-TS) or to a higher level (i.e., SECRET-TS). Sanitized media may be downgraded or declassified with the Customer's approval. Only approved equipment and software may be used to overwrite and degauss magnetic media containing classified information. Each action or procedure taken to overwrite or degauss such media will be verified. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the ISSR, who will coordinate repair or destruction with the Customer. (See Table 1.)

Caution: Overwriting, degaussing, and sanitizing are not synonymous with declassification. Declassification is a separate administrative function. Procedures for declassifying media require Customer approval.

(1) Overwriting Media. Overwriting is a software procedure that replaces the data previously stored on magnetic storage media with a predefine set of meaningless data. Overwriting is an acceptable method for clearing. Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the Customer. The success of the overwrite procedure will be verified through random sampling of the overwritten media. The effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. To clear magnetic disks, overwrite all locations three (3) times (first time with a character, second time with its complement, and the third time with a random character). Items which have been cleared must remain at the previous level of classification and remain in a secure, controlled environment.

(2) Degaussing Media. Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more reliable than overwriting magnetic media. Magnetic media are divided into three types. Type I degaussers are used to degauss Type I magnetic media (i.e., media whose coercivity is no greater than 350 Oersteds (Oe)). Type H degaussers are used to degauss Type 11 magnetic media (i.e., media whose coercivity is no greater than 750 Oe). Currently there are no degaussers that can effectively degauss all

Type HI magnetic media (i.e., media whose coercivity is over 750 Oe). Some degaussers are rated above 750 Oersteds and their specific approved rating will be determined prior to use. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically-saturated material's magnetization to zero. The correct use of degaussing products improves assurance that classified data is no longer retrievable and that inadvertent disclosure will not occur. Refer to the current issue of NSAS ***Information*** Systems ***Security Products and Services Catalogue*** (Degausser Products List Section) for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to ensure continued compliance with the specification NSA CSS ***Media Declassification and Destruction Manual NSA 130-2.***

(3) Sanitizing Media. Sanitization removes information from media such that data recovery using any known technique or analysis is prevented. Sanitizing is a two-step process that includes removing data from the media in accordance with Table 1 and removing all classified labels, markings, and activity logs.

(4) Destroying Media. Data storage media will be destroyed in accordance with Customer-approved methods.

(5) Releasing Media. Releasing sensitive or classified Customer data storage media is a three-step process. First, the Provider will sanitize the media and verify the sanitization in accordance with procedures in this chapter. Second, the media will be administratively downgraded or declassified either by the CSA or the ISSR, if such authority has been granted to the ISSR. Third, the sanitization process, downgrading or declassification, and the approval to release the media will be documented.

Table 1
Clearing and Sanitization Data Storage

Type Media	Clear	Sanitize
(a) Magnetic Tape		
Type I	s o r b	a, b, or destroy
Type II	a o r b	b or destroy
Type III	a o r b	Destroy
(b) Magnetic Disk Packs		
Type I		a, b, or c
Type II		b o r e
Type III		Destroy
(c) Magnetic Disk Packs		
Floppies	a, b, or c	Destroy
Bernoulli's	a, b, or c	Destroy
Removable Hard Disks	a, b, or c	a, b, c, or destroy
Non-Removable Hard Disks	c	a, b, c, or destroy
(d) Optical Disk		
Read Only		Destroy
Write Once, Read Many (Worm)		Destroy
Read Many, Write Many	c	Destroy

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser

b. Degauss with a Type II degausser

c. Overwrite all locations with a character, its complement, then with a random character. Verify that all sectors have been overwritten and that no new bad sectors have occurred. If new bad sectors have occurred during classified processing, this disk must be sanitized by method a or b described above. Use of the overwrite for sanitization must be approved by the Customer.

Note: For hand-held devices (e.g., calculators or personal directories), sanitization is dependent upon the type and model of the device. If there is any question about the correct sanitization procedure, contact the manufacturer or the Customer. In general, sanitization is accomplished as follows: Depress the "CLEAR ENTRY" and the "CLEAR MEMORY" buttons, remove the battery for several hours, and remove all associated magnetic media and retain it in the SAPF or destroy. In some models there are special-purpose memories and key-numbered memories, as well as "register stacks." Caution will be taken to clear all such memories and registers. This may take several key-strokes and may require the use of the operator's manual. Test the hand held device to ensure that all data has been removed. If there is any question, the device will remain in the SAPF or be destroyed.

Table 2
Sanitizing AIS Components

TYPE	PROCEDURE
Magnetic Bubble Memory	a, b, or c
Magnetic Core Memory	a, b, or d
Magnetic Plated Wire	d o r e
Magnetic-Resistive Memory	Destroy
Solid State Memory Components	
Random Access Memory (RAM) (Volatile)	f, then j
Nonvolatile RAM (NOVRAM)	l
Read Only Memory (ROM)	Destroy (see k)
Programmable ROM (PROM)	Destroy (see k)
Erasable Programmable ROM (EPROM)	g, then d and j
Electronically Alterable PROM (EAPROM)	h, then d and j
Electronically Erasable PROM (EEPROM)	i, then d and j
Flash EPROM (FEPROM)	i, then d and j

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser.

b. Degauss with a Type II degausser.

c. Overwrite all locations with any character.

d. Overwrite all locations with a character, its complement, then with a random character.

e. Each overwrite will reside in memory for a period longer than the classified data resided.

f. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.

g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.

h. Pulse all gates.

i. Perform a full chip erase. (See Manufacturer's data sheet.)

j. Check with Customer to see if additional procedures are required.

k. Destruction required only if ROM contained a classified algorithm or classified data.

l. Some NOVRAM are backed up by a battery or capacitor power source; removal of this source is sufficient for release following item f procedures. Other NOVRAM are backed up by EEPROM which requires application of the procedures for EEPROM (i.e., i, then d and j).

Section 6. AIS Acquisition, Maintenance, and Release

S-600. AIS Acquisition, Maintenance, and Release.

a. **Acquisition.** AISS and AIS components that will process classified information will be protected during the procurement process from direct association with the Customer's program, When required by the Customer, protective packaging methods and procedures will be used while such equipment is in transit to protect against disclosure of classified relationships that may exist between the Customer and the Provider.

b. **Maintenance Policy. The** Provider will discuss maintenance requirements with the vendor before signing a maintenance contract. The Customer may require that AISS and AIS components used for processing Customer information will be protected during maintenance from direct association with the Customer's program.

(1) Cleared maintenance personnel are those who have a valid security clearance and access approvals commensurate with the information being processed. Complete sanitization of the AIS is not required during maintenance by cleared personnel, but need-to-know will be enforced. However, an appropriately cleared Provider individual will be present within the SAPF while a vendor performs maintenance to ensure that proper security procedures are being followed. Maintenance personnel without the proper access authorization and security clearance will *always be* accompanied by an individual with proper security clearance and access authorization and never left alone in a SAPF. The escort shall be approved by the ISSR and be technically knowledgeable of the AIS to be repaired.

(2) Prior to maintenance by a person requiring escort, either the device under maintenance shall be physically disconnected from the classified AIS (and sanitized before and after maintenance) or the entire AIS shall be sanitized before and after maintenance. When a system failure prevents clearing of the system prior to maintenance by escorted maintenance personnel, Customer-approved procedures will be enforced to deny the escorted maintenance personnel visual and electronic access to any classified data that may be contained on the system.

(3) All maintenance and diagnostics should be performed in the Provider's secure facility. Any AIS component or equipment released from secure control for any reason may not be returned to the SAPF without the approval of the ISSR. The Customer may require that a permanent set of procedures be in place for the release and return of components. These procedures will be incorporated into the AISSP.

c. Maintenance Materials and Methods.

(1) Unclassified Copy of Operating System. A separate, unclassified, ***dedicated for maintenance*** copy of the operating system (i.e., a specific copy other than the copy(s) used in processing Customer information), including any microcode floppy disks or cassettes that are integral to the operating system, will be used whenever maintenance is done by uncleared personnel. This copy will be labeled "UNCLASSIFIED-FOR MAINTENANCE USE ONLY." Procedures for an AIS using a nonremovable storage device on which the operating system is resident will be considered by the Customer on a case-by-case basis.

(2) Vendor-supplied Software and/or Firmware. Vendor-supplied software and/or firmware used for maintenance or diagnostics will be maintained within the secure computing facility and stored and controlled as though classified. If permitted by the Customer, the ISSR may allow, on a case-by-case basis, the release of certain types of costly magnetic media for maintenance such as disk head-alignment packs.

(3) Maintenance Equipment and Components. All tools, diagnostic equipment, and other devices carried by the vendor to the Provider's facility will be controlled as follows:

(a) Tool boxes and materials belonging to a vendor representative will be inspected by the assigned escort before the vendor representative is permitted to enter the secure area.

(b) The ISSR will inspect any maintenance hardware (such as a data scope) and make a best technical assessment that the hardware cannot access classified data. The equipment will not be allowed in the

secure area without the approval of the ISSR.

(c) Maintenance personnel may bring kits containing component boards into the secure facility for the purpose of swapping out component boards that may be faulty. Any component board placed into an unsanitized AIS will remain in the security facility until proper release procedures are completed. Any component board that remains in the kit and is not placed in the AIS may be released from the secure facility.

(d) Any communication devices with transmit capability belonging to the vendor representative or any data storage media not required for the maintenance visit will be retained outside the SAPF for return to the vendor representative upon departure from the secure area.

(4) Remote Diagnostic Links. Remote diagnostic links require Customer approval. Permission for the installation and use of remote diagnostic links will be requested in advance and in writing. The detailed procedures for controlling the use of such a link or links will have the written approval of the Customer prior to implementation.

d. **Release of Memory Components and Boards.** Prior to the release of any component from an area used to process or store Customer information, the following requirements will be met in respect to coordination, documentation, and written approval. This section applies only to components identified by the vendor or other technically knowledgeable individual as having the capability of retaining user addressable data and does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this document, a memory component is considered to be the ***Lowest Replaceable Unit*** (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module or may consist of several modules and subassemblies. Unlike media sanitization, clearing may be an acceptable method of sanitizing components for release (see 8-501, Table 2). Memory components are specifically handled as either volatile or nonvolatile as described below.

(1) Volatile Memory Components. Memory components that *do not* retain data after removal of all electrical power sources, and when reinserted into a similarly configured AIS *do not* contain residual data, are considered volatile memory components. Volatile components may be released only after accomplishing the following steps:

(a) Maintain a record of the equipment release indicating that all component memory is volatile and that no data remains in/on the component when power is removed.

(b) Equipment release procedures shall be developed by the ISSR and stated in the AISSP.

(2) Nonvolatile Memory Components. Memory components that *do* retain data when all power sources are disconnected are nonvolatile memory components. Nonvolatile memory components defined as ***read only memory*** (ROM), ***programmable ROM*** (PROM), or ***erasable PROM*** (EPROM)that have been programmed at the vendor's commercial manufacturing facility are considered to be unalterable in the field and may be released. Customized components of this nature that have been programmed with a classified algorithm or classified data will be destroyed. All other nonvolatile components may be released after successful completion of the procedures outlined in 8-501, Table 2. Failure to accomplish these procedures will require the ISSR to coordinate with the Customer for a determination of releasability. Nonvolatile components shall be released only after accomplishing the following steps:

(a) Maintain a record of the equipment release indicating the procedure used for sanitizing the component, who performed the sanitization, and who it was released to.

(b) Equipment release procedures must be developed by the ISSR and stated in the AISSP. The record will be retained for 12 months.

(3) Inspecting AIS Equipment. All AIS equipment designated for release will be inspected by the ISSR. This review will ensure that all media including internal disks have been removed.

8-601. **Test Equipment.** The Provider will determine the capability of individual test instruments to collect and process information. If necessary, the manufacturer will be asked to provide this information. A description

of the capabilities of individual test equipment will be provided to the Customer. Security requirements are based on concerns about the capability of the equipment to retain sensitive or classified data. Test equipment with nonvolatile fixed or removable storage media will comply with the requirements of this Supplement and be approved by the Customer for introduction and use in the SAPF. Test equipment with no data retention and no secondary storage does not require Customer approval.

Section 7. Documentation and Training

8-700. Documentation and Training.

a. Provider Documentation. The Provider will develop, publish, and promulgate a corporate AIS security policy, which will be maintained on file by the ISSR.

b. Security Documentation. The Provider will develop and maintain security-related documentation which are subject to review by the Customer as follows:

(1) AISSP. Prepare and submit to the Customer for approval an AISSP in accordance with Customer guidance that covers each AIS which will process information for the Customer. This plan will appropriately reference all other applicable Provider security documentation. In many cases, an AISSP will include information that should not be provided to the general user population. In these cases, a separate **user security** guide will be prepared to include only the security procedures required by the users.

(2) Physical Security Accreditation. Maintain on file the physical security accreditation documentation that identifies the date(s) of accreditation, and classification level(s) for the system device locations identified in the AISSP, and any open storage approvals.

(3) Processing Approval. Maintain on file the Customer's processing approval (i.e., interim approval or accreditation) that specifies the date of approval, system, system location, mode of operation, and classification level for which the AIS is approved.

(4) Memorandum of Agreement. Maintain on file a formal memorandum of agreement signed by all Customers having data concurrently processed by an AIS or attached to the network.

(5) AIS Technical Evaluation Test Plan. As a prerequisite to processing in the compartmented or multilevel mode, develop and submit a ***technical evaluation test plan*** to the Customer for approval. The technical evaluation test plan will provide a detailed description of how the implementation of the operating system software, data management system software, and related security software packages will enable the AIS to meet the compartmented or multilevel mode requirements stated herein. The test plan will also outline the test procedures proposed to demonstrate this compliance. The results of the test will be maintained for the life of the system.

(6) Certification Report. The Certification Report will be maintained for the life of the system.

c. **System User Training and Awareness. All AIS** users, custodians, maintenance personnel, and others whose work is associated with the Customer will be briefed on their security responsibilities. These briefings will be conducted by the Provider. Each individual receiving the briefing will sign an agreement to abide by the security requirements specified in the AISSP and any additional requirements initiated by the Customer. This securit y awareness training will be provided prior to the individual being granted access to the classified AIS and at least annually thereafter. The awareness training will cover the following items and others as applicable:

(1) The security classifications and compartments accessible to the user and the protection responsibilities for each. If the user is a privileged user, discuss additional responsibilities commensurate with those privileges;

(2) Requirements for controlling access to AISS (e.g., ***user lDs, passwords and password security, the need-to-know principle, and protecting terminal screens and printer output from unauthorized access);***

(3) Methods of securing unattended AISs such as checking print routes, logging off the host system or network, and turning the ***A IS off,***

(4) Techniques for securing printers such as removing latent images from laser drums, cleaning platens, and locking up ribbons;

(5) Caution against the use of government-sponsored computer resources for unauthorized applications;

(6) The method of reporting security-related incidents such as misuse, violations of system security, unprotected media, improper labeling, network data spillage, etc.;

(7) Media labeling, including classification labels, data-descriptor labels, placement of labels on media, and maintenance of label integrity;

(8) Secure methods of copying and verifying media;

(9) Methods of safeguarding media, including write protection, removal from unattended AISs, and storage;

(10) Methods of safeguarding hard-copy output, including marking, protection during printing, and storage;

(11) Policy on the removal of media;

(12) Methods of clearing and sanitizing media;

(13) Procedures for destroying and disposing of media, printer ribbons, and AIS circuit boards and security aspects of disposing of AISs;

(14) Methods of avoiding viruses and other malicious code including authorized methods of acquiring software, examining systems regularly, controlling software and media, and planning for emergencies. Discuss the use of recommended software to protect against viruses and steps to be taken when a virus is suspected;

(15) AIS maintenance procedures including the steps to be taken prior to AIS maintenance and the user's point-of-contact for AIS maintenance matters;

(16) Any special security requirements with respect to the user's AIS environment including connections to other AIS equipment or networks;

(17) The use of personally owned electronic devices within the SAPF;

(18) Any other items needed to be covered for the specific Customer's program.